

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-331405

(43)Date of publication of application : 30.11.1999

(51)Int.Cl.

H04M 11/00
G06F 15/02
// G06F 13/00
H04L 9/10

(21)Application number : 10-134755

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 18.05.1998

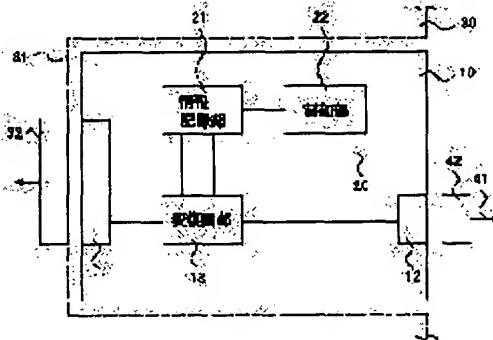
(72)Inventor : MATSUDA MASAYUKI

(54) MODEM CARD AND NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security of communication and the authentication of an opposite party, etc., at the time of remote access.

SOLUTION: This modem card is provided with a first connection terminal part 11 connected to the terminal part 32 of a PCMCIA slot 31, a second connection terminal part 12 connected to the terminal part 42 of an external communication equipment, a modem part 13 for modulating / demodulating communication data between the respective connection terminal parts 11 and 12, an information storage part 21 for storing the communication data modulated or demodulated in the modem part 13 and a control part 22 for controlling access to the information storage part 21. The information storage part 21 and the control part 22 are loaded on a security module 20 and detachably mounted to the modem card 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

特開平11-331405

(43) 公開日 平成11年(1999)11月30日

(51)Int.Cl. ⁶	識別記号	F I
H 0 4 M 11/00	3 0 2	H 0 4 M 11/00
G 0 6 F 15/02	3 3 5	G 0 6 F 15/02
// G 0 6 F 13/00	3 5 3	13/00
H 0 4 L 9/10		H 0 4 L 9/00

F I		
I 0 4 M	11/00	3 0 2
I 0 6 F	15/02	3 3 5 G
	13/00	3 5 3 B
I 0 4 L	9/00	6 2 1 A

審査請求 未請求 請求項の数 7 OL (全 5 頁)

(21)出願番号 特願平10-134755

(71) 出願人 000002897

(22)出願日 平成10年(1998)5月18日

大日本印刷株式会社

東京都新宿区市谷加賀

東京都新宿区市谷加賀町 丁目1番1号
松田 雅之

(72)発明者 松田 雅之

東京都新宿区市谷加

大日本印刷株式会社内

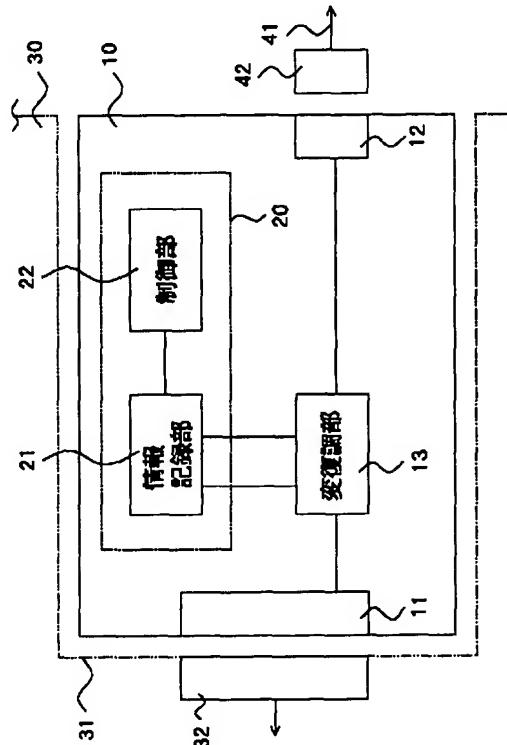
(74) 代理人 奎理士 錢用 久異

(54) 【発明の名称】 モデムカードとネットワークシステム

(57) 【要約】

【課題】 リモートアクセスに際して、通信及び相手の認証等のセキュリティを向上させることを可能にする。

【解決手段】 P C M C I A スロット 3 1 の端子部 3 2 と接続される第 1 の接続端子部 1 1 と、外部通信機器の端子部 4 2 と接続される第 2 の接続端子部 1 2 と、各接続端子部 1 1, 1 2 間の通信データを変調／復調する変復調部 1 3 と、変復調部 1 3 で変調又は復調された通信データを記憶する情報記憶部 2 1 と、情報記憶部 2 1 に対するアクセスを制御する制御部 2 2 とを備え、情報記憶部 2 1 と制御部 2 2 とは、セキュリティモジュール 2 0 に搭載されており、モデムカード 1 0 に取り外し可能に装着される。



【特許請求の範囲】

【請求項1】 携帯型コンピュータのスロットに挿入して使用するモデムカードにおいて、

前記スロットの端子部と接続される第1の接続端子部と、

外部通信機器の端子部と接続される第2の接続端子部と、

前記各接続端子部間の通信データを変調／復調する変復調部と、

前記変復調部で変調／復調された通信データを記憶する情報記憶部と、

前記情報記憶部に対するアクセスを制御する制御部と、を備えたことを特徴としたモデムカード。

【請求項2】 請求項1に記載のモデムカードにおいて、

前記制御部は、データ通信対象コンピュータと間で認証を行う機能を備えたことを特徴とするモデムカード。

【請求項3】 請求項1又は請求項2に記載のモデムカードにおいて、

前記制御部は、前記通信データの暗号化／複合化を行う機能を備えたことを特徴とするモデムカード。

【請求項4】 請求項1から請求項3までのいずれか1項に記載のモデムカードにおいて、

前記制御部及び前記情報記憶部は、セキュリティモジュールに実装していることを特徴とするモデムカード。

【請求項5】 請求項4に記載のモデムカードにおいて、

前記セキュリティモジュールは、取り外し可能であることを特徴とするモデムカード。

【請求項6】 請求項5に記載のモデムカードにおいて、

前記セキュリティモジュールは、SIMカード又はICカードに実装され、そのSIMカード又はICカードが取り外し可能であることを特徴とするモデムカード。

【請求項7】 請求項1から請求項6までのいずれか1項に記載のモデムカードを装着可能な少なくとも1台の携帯型コンピュータと、

前記携帯型コンピュータとの間で通信データの交換を行い、前記制御部との間で認証及び暗号化／複合化を行うホストコンピュータと、を備えたネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、携帯型コンピュータのスロットに挿入して使用するモデムカード及びそのモデムカードを介して接続されたネットワークシステムに関するものである。

【0002】

【従来の技術】 従来、この種のモデムカードは、PDAやパームトップコンピュータといった携帯型コンピュー

10

タのPCMCIAスロットに挿入して使用されており、PHS、携帯電話、公衆電話などの外部通信機器を使用して、公衆回線や専用回線などを介して、ネットワークにアクセスすることができる。システムへのアクセスは、特に、社内システム等でも基幹システム等のセキュリティを要するシステムへの場合には、回線セキュリティの維持、通信相手の確認（認証）等の制約から、Call BackやFire Wall等により、非常に制限されているのが現実である。

【0003】

【発明が解決しようとする課題】 しかし、Call Backの場合には、携帯電話が不正使用（盗難など）されることが考えられ、Fire Wallの場合にも、IDや暗唱番号が漏洩すると、セキュリティを維持できなくなる。

【0004】 また、携帯型コンピュータは、例えば、PDAやパームトップパソコンの場合には、ハードウェア的な制約として、拡張スロットにPCMCIAが1スロットのみという形態のものが多く、このスロットでモデムカードを使用してしまうと、システムの拡張性が失われ、セキュリティの向上が難しかった。

【0005】 本発明は、リモートアクセスに際して、通信及び相手の認証等のセキュリティを向上させることができるモデムカードとネットワークシステムを提供することを課題とする。

【0006】

【課題を解決するための手段】 前記課題を解決するためには、請求項1の発明は、携帯型コンピュータのスロットに挿入して使用するモデムカードにおいて、前記スロットの端子部と接続される第1の接続端子部（11）と、外部通信機器の端子部と接続される第2の接続端子部（12）と、前記各接続端子部間の通信データを変調／復調する変復調部（13）と、前記変復調部で変調／復調された通信データを記憶する情報記憶部（21）と、前記情報記憶部に対するアクセスを制御する制御部（22）と、を備えたことを特徴としたモデムカードである。

【0007】 請求項2の発明は、請求項1に記載のモデムカードにおいて、前記制御部は、データ通信対象コンピュータと間で認証を行う機能を備えたことを特徴とするモデムカードである。

【0008】 請求項3の発明は、請求項1又は請求項2に記載のモデムカードにおいて、前記制御部は、前記通信データの暗号化／複合化を行う機能を備えたことを特徴とするモデムカードである。

【0009】 請求項4の発明は、請求項1から請求項3までのいずれか1項に記載のモデムカードにおいて、前記制御部（22）及び前記情報記憶部（21）は、セキュリティモジュール（20）に実装していることを特徴とするモデムカードである。

50

【0010】請求項5の発明は、請求項4に記載のモデムカードにおいて、前記セキュリティモジュールは、取り外し可能であることを特徴とするモデムカードである。

【0011】請求項6の発明は、請求項5に記載のモデムカードにおいて、前記セキュリティモジュールは、S I Mカード(20A)又はI Cカード(20B)に実装され、そのS I Mカード又はI Cカードが取り外し可能であることを特徴とするモデムカードである。

【0012】請求項7の発明は、請求項1から請求項6までのいずれか1項に記載のモデムカードを装着可能な少なくとも1台の携帯型コンピュータ(30)と、前記携帯型コンピュータとの間で通信データの交換を行い、前記制御部との間で認証及び暗号化/複合化を行うホストコンピュータ(51)と、を備えたネットワークシステムである。

【0013】

【発明の実施の形態】以下、図面などを参考しながら、本発明の実施の形態をあげて、さらに詳細に説明する。図1は、本発明によるモデムカードの実施形態を示すブロック図、図2は、本発明によるネットワークシステムの実施形態を示す概念図である。この実施形態のモデムカード10は、通常のPCMCIAモデム機能と、I Cカードと同等の機能とを備えるものあって、図1に示すように、PCMCIAスロット31の端子部32と接続される第1の接続端子部11と、外部通信機器の端子部42と接続される第2の接続端子部12と、各接続端子部11、12間の通信データを変調/復調する変復調部13と、変復調部13で変調又は復調された通信データを記憶する情報記憶部21と、情報記憶部21に対するアクセスを制御する制御部22とを備えている。情報記憶部21と制御部22とは、セキュリティモジュール20に搭載されており、モデムカード10に取り付けられている。

【0014】このモデムカード10は、図2に示すように、パームトップパソコン30に設けられたPCMCIAスロット31に装着してその端子部32に第1の接続端子部11を接続し、PHS40に装着される接続コード41の端子部42に第2の接続端子部12を接続して使用される。PHS40は、PHSアンテナ43によって、公衆回線やISDN等の通信手段60を介して、社内LAN50に接続されている。社内LAN50内では、ホストコンピュータ51に、モデム52等を介して、接続されている。

【0015】得意先や移動中に、社外から社内LAN50へのアクセスは、携帯型コンピュータ30を使用して行われる。この場合に、セキュリティ上の対策が必要となっていた。例えば、なりすましや盗聴等の可能性がある。そこで、上記のような接続に際して、セキュリティを高めるために、本実施形態のモデムカード10は、セ

キュリティモジュール20を搭載し、セキュリティを必要とする通信データをガードするようにしたものである。本実施例では、PHSを例にしたが、他の通信手段として、携帯電話、公衆電話等の一般回線を使うこともできる。

【0016】図3は、本実施形態によるモデムカードの実装例を示す図である。図3(a)のモデムカード10Aは、セキュリティモジュールとして、S I Mカード20Aを用いたものであり、図3(b)のモデムカード10Bは、セキュリティモジュールとして、I Cカード20Bを用いたものであり、S I Mカード20A、I Cカード20Bは、カード本体から取り外すことができる。このようにセキュリティモジュールとしてのS I Mカード20A、I Cカード20Bは、取り外し可能な媒体であるので、保管時は、モデムカード10とセキュリティモジュール20を個別に管理でき、トラブル発生時(紛失盗難等)の悪用を防ぐことができる。

【0017】図4は、本実施形態によるモデムカードとネットワークシステムの動作を説明する図である。このモデムカード10は、パームトップパソコン30に装着されており、パームトップパソコン30は、モデムカード10のセキュリティモジュール20との間での認証を行うことにより、モデムカード10の利用者を、常に特定することが可能となる(#101)。次に、通信時に、モデムカード10とホストコンピュータ50(又はAP)との間で、内部認証・外部認証を行うことにより、パームトップパソコン30(モデムカード10)が正当な端末であることを認証する(#102)。

【0018】次に、重要な通信データaを通信する場合に(#103)、送信時に、セキュリティモジュール20内で暗号化して送信し(#104)、受信時には、電文をセキュリティモジュール20で復号化し(#105)、パームトップパソコン30で表示、加工することを可能とする。また、暗号チェックサム(取引認証コード・メッセージ認証コード等)を使用することにより、伝送途中の改ざんを防止することができる。

【0019】なお、パームトップパソコン30は、通常の通信データbの場合には、平文で通信を行うこともできる(#106)。

【0020】以上説明したように、本実施形態のモデムカードは、PDAやサブノート等の携帯型コンピュータのPCMCIAのスロットに装着して使用される。具体的には、モデムカード10に、S I Mカード20A又はI Cカード20Bなどのセキュリティモジュール20を装着して、その暗号化機能で通信を暗号化したり、相互認証という暗号の鍵を外に出さずに、両者の正当性を確認する手法等を用いて、なりすましを防ぐことができる。

【0021】また、セキュリティモジュール20を取り外しできるので、パームトップパソコン30のみを盗ま

れたり、置き忘れても、LANに接続するための鍵は、モデムカード10の中にあるので、安全である。

【0022】以上説明した実施形態に限定されることはなく、種々の変形や変更が可能であって、それらも本発明の均等の範囲内である。例えば、セキュリティモジュールは、社員証やクレジットカードとして併用することができる。また、有料情報通信での電子現金による課金（プリペイド）や、イベント・施設等の予約についても、認証や決済が可能である。

[0023]

【発明の効果】以上詳しく述べたように、本発明によれば、モデムカードにセキュリティモジュールを設けたので、ネットワーク上での認証が可能となり、データセキュリティの向上を図ることができる。また、セキュリティモジュール内で、通信時にデータを暗号化／複合化することができるので、通信のセキュリティをさらに向上させることができる。

【図面の簡単な説明】

【図1】本発明によるモデムカードの実施形態を示すブロック図である。

【図2】本発明によるネットワークシステムの実施形態

を示す概念図である。

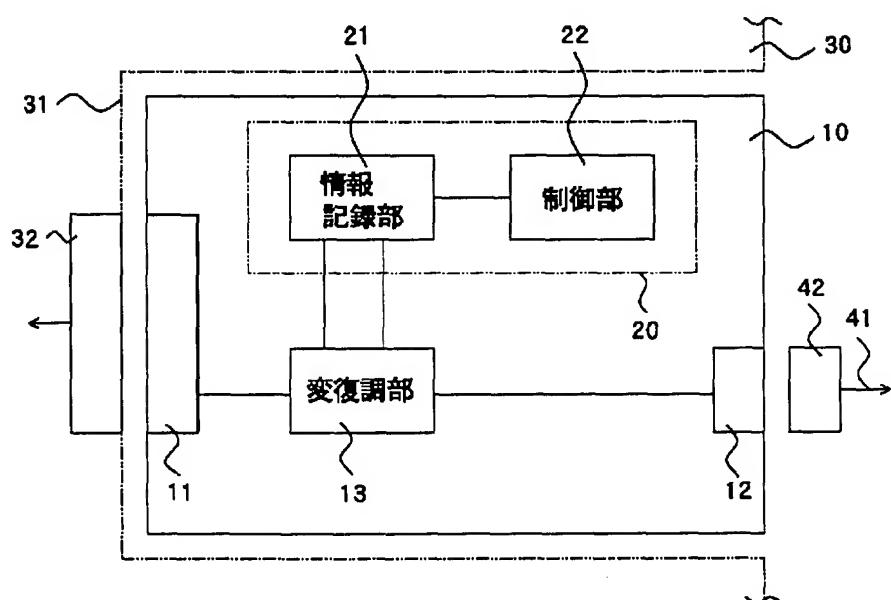
【図3】本実施形態によるモジュールカードの実装例を示す図である。

【図4】本実施形態によるモデムカードとネットワークシステムの動作を説明する図である。

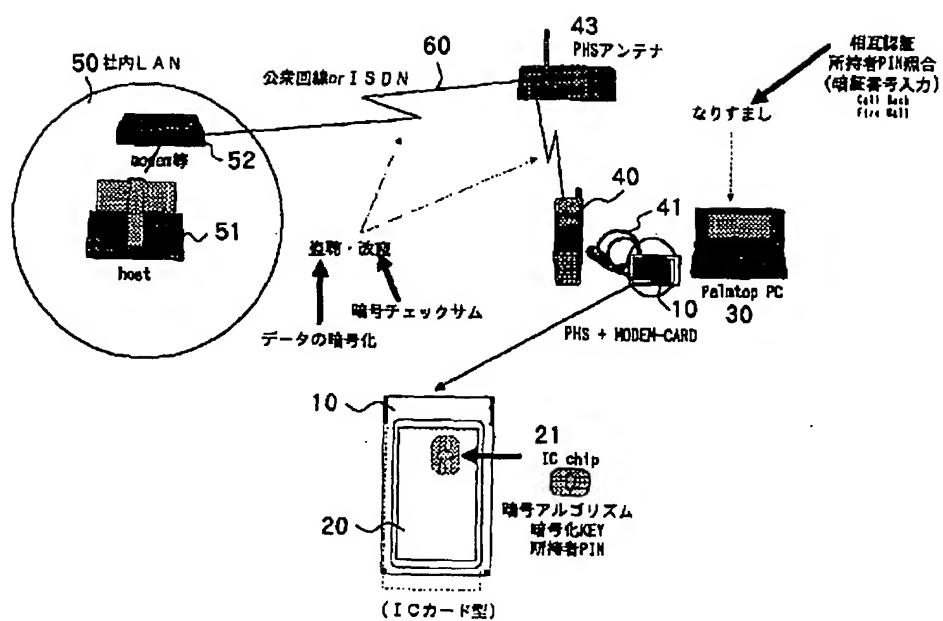
【符号の説明】

1 0	モデムカード
1 1	第 1 の接続端子部
1 2	第 2 の接続端子部
<i>10</i> 1 3	変復調部
2 0	セキュリティモジュール
2 0 A	S I Mカード
2 0 B	I Cカード
2 1	情報記憶部
2 2	制御部
3 0	パームトップパソコン
4 0	P H S
5 0	社内L A N
5 1	ホストコンピュータ
<i>20</i> 6 0	通信手段

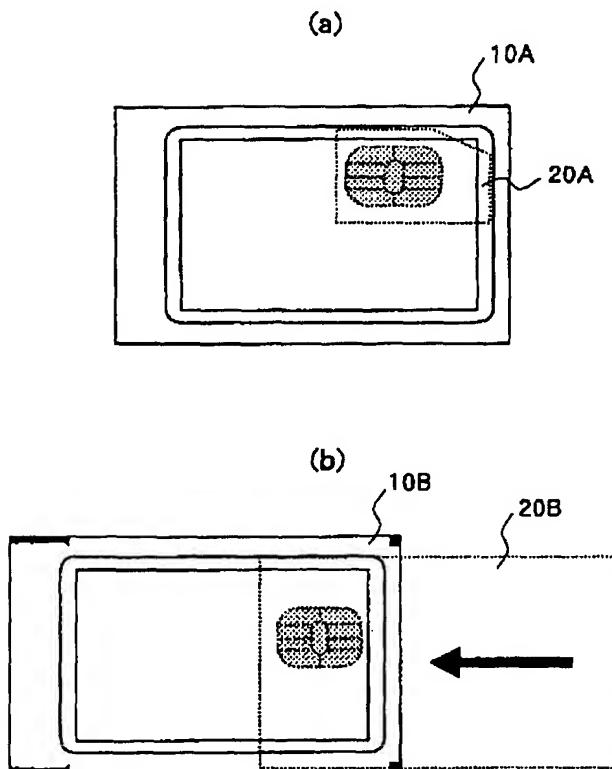
[図 1]



【図2】



【図3】



【図4】

